INTELLIGENCE SUPPORT TO SUPPLY CHAIN RISK MANAGEMENT

GRADUATE RESEARCH PAPER

Charles L. Carter, Major, USAF
AFIT/IOA/ENS/12-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A.
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this graduate research paper are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/IOA/ENS/12-02

INTELLIGENCE SUPPORT TO SUPPLY CHAIN RISK MANAGEMENT

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Analysis

Charles L. Carter, MA

Major, USAF

June 2012

DISTRIBUTION STATEMENT A.
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT/IOA/ENS/12-02

INTELLIGENCE SUPPORT TO SUPPLY CHAIN RISK MANAGEMENT

Charles L. Carter, MA
Major, USAF

Approved:

_____/signed/_____	_____
Daniel D. Mattioda, Major, USAF, Ph.D. (Advisor)	date

Abstract

The purpose of this research was to improve defense supply chain risk management processes through better intelligence integration. To this end, this research sought to capture the present state of academic and Department of Defense (DoD) thought regarding supply chain resiliency and risk management through an extensive review of current academic and DoD literature regarding supply chain risk management and intelligence doctrine. This review established the importance of supply chain risk analysis to ensuring supply chain resiliency and identified a significant gap in DoD acquisitions policy and guidance regarding intelligence support to supply chain risk analysis.

This research culminated in the development of a methodology for intelligence professionals to use to support supply chain risk management processes. Specifically, this paper provides analysts a methodology to provide intelligence support to risk analysis for United States Air Force (USAF) weapon system supply chains based on the Intelligence Preparation of the Operational Environment process established in Joint doctrine. While the methodology developed in this paper is targeted at USAF weapon system supply chains, it is readily adaptable to other DoD acquisitions program supply chains. Additionally, this paper provides recommendations for future research to further improve intelligence support to supply chain risk management.

Acknowledgments

I would like to express my sincere thanks to my research advisor, Maj Daniel Mattioda, Ph.D., for his guidance and support throughout this research effort. Additionally, I would like to thank my sponsor, Lt Col Steven Gorski, commander of the Air Force Material Command Intelligence Squadron and his team for their insight and support throughout this research endeavor. I would also like to thank the numerous faculty members who lend their valuable time to advise and guide me in this effort.

Table of Contents

Table of Figures

Table of Tables

Table of Equations

INTELLIGENCE SUPPORT TO SUPPLY CHAIN RISK MANAGEMENT

I. Introduction

Background

Supply chain risk management has become an important management task in recent years. Trends such as globalization and lean manufacturing have simultaneously lengthened the supply chains of U.S. companies and increased the brittleness of those chains (Pettit, Fiksel, and Croxton, 2010; Giunipero and Eltantawy, 2004). Attempts to minimize costs to remain competitive have trimmed the capacity of manufacturers around the world and resulted in consolidation in many industries. These trends have led to increased sole-sourcing of components in many supply chains and eliminated the capacity necessary to overcome unforeseen events such as natural disasters and political and/or military conflicts (Haywood and Peck, 2004). The trends and their impacts have been especially significant in the U.S. defense industry where they have been accelerated by the pressures of decreasing defense budgets, limited procurement of weapon systems, and export controls limiting manufacturers' access to foreign markets. Additionally, a reduction in U.S. manufacturing capability and increased pressure for defense contractors to lower costs has led to increased out-sourcing of critical parts to foreign manufacturers. This exposes US military forces to a new asymmetric threat as it allows foreign states or non-state actors to intentionally inject sub-standard or intentionally altered parts into DoD supply chains. For example, foreign-manufactured counterfeit parts have been identified in defense industry supply chains exposing the DoD to unknown risk (Associated

Press, 2011; Kendall, 2012). The criticality of developing and maintaining resilient supply chains is recognized at the highest levels of the U.S. government and in January 2012, President Obama released his National Security Strategy for Global Supply Chain Security (President of the United States, 2012). This strategy highlights the President's goals of promoting economic prosperity and national security by ensuring the "secure and efficient movement of goods" and fostering resilient supply chains.

The increasing length and delicacy of manufacturers' supply chains entails risk not only for those manufacturers, but also for the customers who rely on their products. For the U.S. Department of Defense (DoD), this risk is significant as key U.S. military weapon systems such as fighter aircraft, tanks, Intelligence, Surveillance, and Reconnaissance (ISR) systems, and their associated components, are generally produced by a single prime contractor in relatively limited numbers. In the event of a disruption to the prime contractor's supply chain, there are typically few, if any, alternative sources of supply and the alternatives that do exist are both expensive and of limited capacity.

Purpose

Given the potential risks which would accompany a significant disruption of a major DoD weapon system supply chain, it is imperative that the DoD and the services improve their supply chain risk management procedures. While this problem has been identified by the DoD and efforts have been made to increase the rigor of supply chain risk management processes in the department, there remains a lack of guidance regarding the intelligence community's role in managing supply chain risk. To help fill this gap and assist in developing policies and

techniques to improve intelligence support to supply chain risk management, this paper is intended to provide staff officers with a methodology for identifying, assessing, monitoring, and mitigating risk to U.S. Air Force (USAF) weapon systems' supply chains through enhanced intelligence support.

Methodology

In order to develop a practical methodology for intelligence personnel to use to support supply chain risk management for USAF weapon systems, this paper first seeks to build a foundation of understanding with regard to the relevant academic concepts and DoD practices. To this end, the paper begins with an in-depth review of the academic concepts and literature relating to supply chain risk. Following this review, we conduct a study of the current DoD and USAF guidance regarding supply chain risk management to gain an understanding of how intelligence currently supports these processes and the specific policies in place governing that support. With a sound understanding of current academic theory and DoD practice, this paper proposes a grounded methodology for providing intelligence support to USAF supply chain risk management processes.

II. Literature Review

Overview

While this paper focuses on the role of intelligence in supply chain risk analysis, it is important to first gain an understanding of supply chain resiliency, the associated concepts, and the process of improving resiliency through risk management.

According to Pettit, Fiksel, and Croxton (2010:6), a supply chain is "the network of companies involved in the upstream and downstream flows of products, services, finances, and information from the initial supplier to the ultimate customer." This definition closely follows that of Peck who asserts a supply chain is "the network of organizations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer" (Peck, 2005a:210-11). Lambert and Cooper (2000:66) emphasize the management of business processes across the supply chain in their research and define supply chain management as "the integration of key business processes from end-users to original suppliers that provide products, services and information that add value for customers and other stakeholders." Because of the complex and interwoven nature of the relationships between the organizations and the processes that comprise a supply chain and the effects of an uncertain external environment, supply chains are vulnerable to disruption (Pettit, Fiksel,and Croxton, 2010). In order to measure and overcome their supply chains' susceptibility to disruption and the associated productivity and profit losses that typically follow a disruption, managers and academics have developed the concept of supply chain resiliency.

Supply Chain Resiliency

From a review of the relevant literature, supply chain resiliency is commonly defined as the "capacity for an enterprise to survive, adapt, and grow in the face of turbulent change" (Fiksel, 2006:16). Alternatively, Christopher and Peck (2004a:2) define resiliency as the "ability of a system to return to its original state or move to a new, more desirable state after being disturbed." In USAF operations, this concept is referred to as an organization's ability to survive and operate (Department of the Air Force, 1998). All complex organizations, just as other complex systems like ecosystems, have a certain level of resiliency (Pettit, 2008). Like an ecosystem, an organization's resiliency allows it to successfully survive, adapt and potentially flourish in the face of change, or if the organization is insufficiently resilient in the face of change, results in the organization's failure to adapt and thus, its eventual demise (Peck, 2005a). As change is a constant in both the business and military environments, resiliency is a key determinant of an organization's success or failure in these environments. Like businesses, military organizations rely on a steady flow of the products and services necessary for them to operate and provide value to their stakeholders. As a result of this reliance, it can be argued that any organization can only be as resilient as the supply chain that supports it (Pettit, 2008).

Blackhurst, Dunn, and Craighead (2011) investigated supply chain resiliency factors using systems theory and a resource-based view of a firm's operations. Based on systems theory, they assert organizations function as open systems and require "a steady flow of inputs that originate and are extracted from sources in the environment to sustain their operations" (Blackhurst, Dunn, and Craighead, 2011:375). As open systems, organizations have flows (activities associated with extracting inputs from the environment), flow units (the specific inputs

from the environment such as raw materials or semi-finished goods), sources (the supply node providing the input). Disruptions to the flow of inputs in the system impact the firm's ability to operate.

From the resource-based view of the firm, Blackhurst, Dunn, and Craighead (2011) approach the firm as a collection of resources and capabilities which result in the firm's performance. Resources, both tangible and intangible, provide "capabilities that determine how firms react to various internal and external threats and opportunities" (Blackhurst, Dunn, and Craighead: 2011:376). Using this view of the firm, the author's categorize their findings into three categories: 1) Physical Capital Resources, 2) Human Capital Resources, and 3) Organizational and Interorganizational Capital Resources. The interaction and coordination of these resource categories determine the firm's ability to mitigate supply chain disruptions.

From their investigation, Blackhurst, Dunn, and Craighead (2011) developed six empirical generalizations regarding supply chain resiliency. Three of these generalizations relate to factors which enhance supply chain resiliency and three relate to factors which reduce resiliency. In addition, under the category of each generalization, the authors have identified specific factors which are either positively or negatively related to supply chain resiliency (Blackhurst, Dunn, and Craighead, 2011). Their specific findings are outlined in Table 1.

Supply Chain Resiliency Enhancers		
1. Human capital enhancers are positively related to supply resiliency		
Supply chain education and training	Understanding Cost/benefit trade-offs	Post-disruption feedback (lessons learned)
2. Organizational and interorganizational capital enhancers are positively related to supply resiliency		
Defined communication networks	Cross-functional risk management teams	Developing and practicing contingency plans
Partnering with customs programs and developing port diversification plans	Developing supplier relationship management programs	
3. Physical capital enhancers are positively related to supply resiliency		
Safety stock	Supply chain visibility	Monitoring systems and other preventive risk tools
The ability to monitor risk at individual nodes in the chain	The ability to quickly redesign a supply chain	
Supply Chain Resiliency Reducers		
4. Flow activity reducers are negatively related to supply resiliency		
The number of nodes (higher is less resilient)	Stringent security and customs regulations	Port and vessel capacity restrictions
5. Flow unit reducers are negatively related to supply resiliency		
Product complexity	Stringent storage and quality requirements	
6. Source reducers and negatively related to supply resiliency		
The volatility of a supplier's location and supplier clusters	Limitations on supplier capacity	

Table 1 – Supply Chain Resiliency Framework (Blackhurst, Dunn, and Craighead, 2011)

According to Pettit, Fiksel and Croxton (2010), an organization or supply chain's resilience is determined by two constructs: its capabilities and its vulnerabilities. Capabilities are defined as "attributes that enable an enterprise to anticipate and overcome disruptions" (Pettit, 2008:18). Factors impacting capability are identified and described in the Table 2.

Capability Factor	Definition	Sub-Factors
Flexibility in Sourcing	Ability to quickly change inputs or the mode of receiving inputs	Part commonality, Modular product design, Multiple uses, Supplier contract flexibility, Multiple sources
Flexibility in Order Fulfillment	Ability to quickly change outputs or the mode of delivering outputs	Alternate distribution channels, Risk pooling/sharing, Multi-sourcing, Delayed commitment/Production postponement, Inventory management, Re-routing of requirements
Capacity	Availability of assets to maintain sustained production levels	Reserve capacity, Redundancy, Backup energy sources and communications
Efficiency	Capability to produce outputs with minimum resource requirements	Waste elimination, Labor productivity, Asset utilization, Product variability reduction, Failure prevention
Visibility	Knowledge of status of operating assets and the environment	Business intelligence gathering, Information technology, Product, equipment, and people visibility, Information exchange
Adaptability	Ability to modify operations in response to challenges or opportunities	Fast re-routing of requirements, Lead time reduction, Strategic gaming and simulation, Seizing advantage from disruptions, Alternative technology development, Learning from experience
Anticipation	Ability to discern potential future events or situations	Monitoring early warning signals, Forecasting, Deviation and near-miss analysis, Risk management, Business continuity/preparedness planning
Recovery	Ability to return to normal operations state rapidly	Crisis management, Resource mobilization, Communications strategy, Consequence mitigation
Dispersion	Broad distribution or decentralization of assets	Distributed decision-making and Assets, Decentralization of key resources, Location-specific empowerment, Dispersion of markets
Collaboration	Ability to work effectively with other entities for mutual benefit	Collaborative forecasting, Customer management, Communications, Postponement of orders, Product life cycle management, Risk sharing with partners
Organization	Human resource structures, policies, skills and culture	Accountability, Creative problem-solving, Cross training, Substitute leadership/empowerment, Learning/benchmarking, Culture of caring
Market Position	Status of a company or its products in specific markets	Product differentiation, Customer loyalty/retention, Market share, Brand equity, Customer relationships, Customer communications
Security	Defense against deliberate intrusion or attack	Layered defenses, Access restrictions, Employee involvement, Collaboration with governments, Cyber-security, Personnel security
Financial strength	Capacity to absorb fluctuations in cash flow	Insurance, Portfolio diversification, Financial reserves and liquidity, Price margin

Table 2 – Supply Chain Capabilities (Pettit, 2008)

Vulnerabilities are defined as "attributes which make an organization susceptible to disruptions" (Pettit, 2008:44). Factors impacting vulnerability are identified and described in the Table 3.

Vulnerability Factor	Definition	Sub-Factors
Turbulence	Environment characterized by frequent changes in external factors beyond your control	Natural disasters, Geopolitical disruption, Unpredictability of demand, Fluctuations in currencies and prices, Technology failures, Pandemic
Deliberate threats	Intentional attacks aimed at disrupting operations or causing human or financial harm	Theft, Terrorism/sabotage, Labor disputes, Espionage, Special interest groups, Product liability
External pressures	Influences, not specifically targeting the firm, that create business constraints or barriers	Competitive innovation, Social/Cultural change, Political/Regulatory change, Price pressures, Corporate responsibility, Environmental change
Resource limits	Constraints on output based on availability of the factors of production	Supplier, Production and Distribution capacity, Raw material and Utilities availability, Human resources
Sensitivity	Importance of carefully controlled conditions for product and process integrity	Complexity, Product purity, Restricted materials, Fragility, Reliability of equipment, Safety hazards, Visibility to stakeholders, , Symbolic profile of brand, Concentration of capacity
Connectivity	Degree of interdependence and reliance on outside entities	Scale of network, Reliance upon information, Degree of outsourcing, Import and Export channels, Reliance upon specialty sources
Supplier/Customer disruptions	Susceptibility of suppliers and customers to external forces or disruptions	Supplier reliability, Customer disruptions

Table 3 – Supply Chain Vulnerabilities (Pettit, 2008)

Whereas the capabilities identified by Pettit are determined by the members of the supply chain, the vulnerabilities identified are largely driven by external factors such as suppliers, the

requirements of the output product or service with regards to input specifications, and customer demand. These vulnerabilities constitute potential disruptions to the supply chain. In the larger supply chain literature, these potential disruptions are referred to as risks.

Supply Chain Risk

According to the Merriam-Webster dictionary, a risk is defined as a "possibility of loss or injury." Alternatively, risk is also defined as "someone or something that creates or suggests a hazard" (Merriam-Webster). Manuj and Mentzer (2008b:197-98) define supply risk as "the distribution of outcomes related to the adverse events in inbound supply that affect the ability of the focal firm to meet customer demand (in terms of both quantity and quality) within anticipated costs and time, or causes threats to customer life and safety." Based on this definition and supply chain risk literature, for the purposes of this paper, risk will be defined as the "level of exposure to uncertainties that the enterprise must understand and effectively manage to…achieve its…objectives and create value" (Norrman and Jansson, 2004:436). Risks are posed by specific events which are referred to as risk events.

A review of the relevant literature indicates that risk has two components: 1) impact of an event, and 2) probability of the event occurring (Manuj and Mentzer, 2008b; Norrman and Jansson, 2004). In the intelligence community, risk is closely associated with the concept of threat in that a threat is identified as an adversary's capability and intent to damage, disrupt or destroy friendly forces (Joint Chiefs of Staff, 2007). However, the concept of risk in supply chain literature extends beyond the intelligence community's term "threat" to incorporate not

only potential actions that may be taken by a competitor, but also risks posed by the environment itself such as changes in supply and demand.

A review of supply chain risk literature suggests four broad categories of risk: supply, demand, operational and security risks (Christopher and Lee, 2004a; Manuj and Mentzer, 2008a; Manuj and Mentzer, 2008b). Operations risk is defined as the probability "distribution of outcomes related to adverse events within the firm that affect a firm's internal ability to produce goods and services, quality and timeliness of production, and/or profitability" (Manuj and Mentzer, 2008:198). Demand risk is identified as "the distribution of outcomes related to adverse events in the outbound flows that affect the likelihood of customers placing orders with the focal firm, and/or variance in the volume and assortment desired by the customer" (Manuj & Mentzer, 2008:198). Finally, security risk is the "distribution of outcomes related to adverse events that threaten human resources, operations integrity, and information systems; and may lead to outcomes such as freight breaches, stolen data or proprietary knowledge, vandalism, crime and sabotage" (Manuj and Mentzer, 2008:198).

Alternatively, Ghoshal (1987) suggests classifying risks into the following four categories based on their source:

1. Macroeconomic risks associated with significant economic shifts in wage rates, interest rates, exchange rates, and prices
2. Policy risks associated with unexpected actions of national governments
3. Competitive risks associated with uncertainty about competitor activities in foreign markets

4. Resource risks associated with unanticipated differences in resource requirements in foreign markets (Manuj and Mentzer, 2008b).

Manuj and Mentzer (2008b:198) assert that risk events in both domestic and global supply chains are inter-woven in complex ways with "one risk leading to another, or influencing the outcome of other risks." Additionally, while this complexity exists in domestic supply chains, the "unpredictability and impact of these complex relationships increases in global supply chains" due to increased uncertainty in lead times, transit times, product quality, forecasting, international politics, politics in the supplier's host country and other factors (Manuj and Mentzer, 2008b:198).

Supply Chain Risk Management

Manuj and Mentzer (2008b) define risk management as the process of identifying and understanding risks and taking appropriate actions to cost-effectively mitigate the potential impacts of those risks on the supply chain. Alternatively, Haywood and Peck (2004:7) suggest supply chain risk management should be defined as "the identification and management of risks within the supply chain and risks external to it through a coordinated approach amongst supply chain members to reduce supply chain vulnerability as a whole." Generally, risk management involves identifying and evaluating all potential outcomes of a process or event and then comparing the potential gains with the potential losses or risks (Pettit, Fiksel, and Croxton, 2010). Risk mitigation strategies must balance the likelihood and potential impacts of risk events with the costs of transferring the risks, avoiding the risks, or reducing their impacts

(Manuj and Mentzer, 2008a). Because the environment in which the supply chain operates and the supply chain itself are constantly evolving and changing, risk management is a continuous process (Pettit, Fiksel, and Croxton, 2010).

One critique of traditional risk management techniques is that they assume that all potential risks are knowable and thus can be identified and evaluated (Pettit, Fiksel, and Croxton, 2010). However, in practice this is not usually realistic and managers must compensate for these unforeseen events by enhancing the resilience of their supply chains outside the risk management process. With this limitation in mind, risk management still provides a useful method for proactively enhancing supply chain resiliency.

Based on a review of the relevant literature, an adapted six-step supply chain risk management process is provided below (Norrman and Jansson, 2004; Pettit, 2008; Pettit, Fiksel, and Croxton, 2010):

1. Identify threats and hazards to the supply chain
2. Assess risks
3. Analyze potential mitigation strategies
4. Select mitigation strategies
5. Implement mitigation strategies
6. Monitor and re-evaluate

Although this process is broken into six steps, steps one and two are generally treated as one in the literature and referred to as supply chain risk analysis. Risk analysis is the process of identifying and understanding the risks to a supply chain (Manuj and Mentzer, 2008b). To analyze risk, managers must not only identify potential risk events and their potential impacts,

but also understand the potential sources and causes of those risks so that their likelihood and the circumstances which impact their likelihood can be determined (Manuj and Mentzer, 2008b). Risk analysis allows managers to assess and prioritize risks in order to efficiently and effectively allocate resources to mitigate them.

Peck suggests a multi-level framework for supply chain risk analysis consisting of four levels or perspectives. Peck asserts these levels are inextricably linked as elements of the supply chain system, but can be usefully separated to guide analysis. The levels are: Level 1 – value stream/product or process, Level 2 – assets and infrastructure dependencies, Level 3 – organizations and interorganizational networks, and Level 4 – the environment (Peck, 2005a).

At Level 1, supply chain vulnerability is evaluated from an "engineering-based supply chain management perspective" (Peck, 2005a:219). From this perspective, the supply chain is viewed as a "logistics pipeline flowing through and between organizations within the network" (Peck, 2005a:219). In this level, analysts should examine the supply chain to identify seams between organizations especially with regard to information flow. Using this approach, risks are primarily the "financial or commercial consequences of inefficiencies or sub-optimal supply chain performance, including the inability to react swiftly to volatility in demand and the changing needs of the market" (Peck, 2005a:219).

At Level 2, the supply chain is examined "in terms of the assets and infrastructure needed to produce and carry the goods and information flows" identified in level 1(Peck, 2005a:219). This perspective reflects a physical evaluation of the nodes (e.g. factories, distribution centers, retail outlets, etc.) and links (e.g. roads, pipelines, power grids, rail, waterways, telecommunication networks, shipping lanes, etc.) where goods, services, and information are

created or through which they are transported. In Level 2, the vulnerability of the network should be assessed in terms of the probabilities and impacts of the "loss of links, nodes, and other essential operating assets" to include skilled workers (Peck, 2005a:220).

In Level 3, the supply chain is viewed as an "inter-organizational network" (Peck, 2005a:220). From this perspective, the nodes in the network are the firms and organizations which "own or manage the assets and infrastructure, through which the physical goods and information flow" and the links are the relationships, both formal and informal, between these organizations (Peck, 2005a:221). At Level 3, the dependencies between organizations and their relative power to set the terms of their relationships is examined to identify linkages which might subject the supply chain to risk.

In Level 4, the "wider macroeconomic and natural environment" in which the supply chain and its nodes and links exist is evaluated (Peck, 2005a:223). At this level, the potential impacts of man-made forces such as political, economic, social, and technological forces as well as natural forces such as geology, ecology, pathology, and weather are identified and analyzed (Peck, 2005). Because global supply chains exist within a broad environment spanning many countries, cultures, climates, and geographic regions, environmental impacts can have significant and often unanticipated impacts on a supply chain (Peck, 2005).

Norrman and Jansson (2004) suggest a similar approach to risk analysis based on their research of Ericsson's supply chain risk management process. Ericsson's current risk management practices were developed after the firm suffered a significant supply chain disruption and resulting profit loss due to a fire in March 2000 at a sub-supplier's plant in New Mexico. This plant was the sole producer of a microchip used in one of Ericsson's key consumer

products and as a result of the disruption, the firm lost several months of mobile phone production with total losses from the disruption calculated at approximately $200 million (Norrman and Jansson, 2004).

As a result of these losses, Ericsson adopted a robust risk management process consisting of a continuous cycle with six steps: 1) Risk Identification, 2) Risk Assessment, 3) Risk Treatment/Management, 4) Risk Monitoring and Follow-Up, 5) Incident Handling and 6) Business Continuity Planning. For the purposes of understanding the firm's risk analysis processes, this paper will focus on steps 1 and 2 of this process. The firm's approach to risk analysis is cross-functional and relies on a risk management council with members from corporate risk management, contracting and purchasing functions, supply chain managers and logistics functions, product manufacturing and distribution process owners, and marketing and sales (Norrman and Jansson, 2004). The importance of a cross-functional approach to supply chain management in general and risk analysis in particular has been highlighted by several researchers in supply chain management and is a key component of Ericsson's risk management strategy (Blackhurst, Dunn, and Craighead, 2011; Lambert and Cooper, 2000; Norrman and Jansson, 2004).

In its risk identification step, Ericsson first identifies and analyzes its supply chain risks by mapping the upstream supply chain, evaluating suppliers and their products and services (Norrman and Jansson, 2004). In this step, the firm seeks to identify the flow of products, services and information to and from its suppliers and define the critical parts and risk sources in its processes. The purpose of this analysis is to determine the risks to the firm of a disruption based on the likelihood and impact of a given risk event (Norrman and Jansson, 2004). Each

component required in its products is first classified based on the availability of sources. The classifications are as follows:

1. The product is currently sourced from more than one approved source (e.g. two or more manufacturers or one manufacturer with two or more sites)
2. The product is currently sourced from one approved source; other sources are approved and available, but are not used
3. The product is currently sourced from one approved source; other sources are approved and available, but no tools, masks, or other equipment needed for production are in place
4. The product is currently sourced from one supplier. No additional manufacturer is available

   (Norrman and Jansson, 2004)

After classifying each component based on availability of sources, Ericsson classifies them based on how long a disruption will affect deliveries of the component. This classification is referred to as the risk event's business recovery time (BRT). The classifications of BRT are as follows:

1. It takes less than three months to get deliveries from an alternative source
2. Three to eight months to get approval and deliveries from an alternative source
3. Nine to 12 months or product is unavailable and must be re-designed
4. Twelve months or more or product unavailable and must be re-designed. Component that must be re-designed is highly complex

   (Norrman and Jansson, 2004)

After identification and classification of critical components, Ericsson assesses these risks through a thorough analysis of the suppliers and sub-suppliers of these components (Norrman and Jansson, 2004). To evaluate suppliers and sub-suppliers, the firm considers several factors: business control, financial condition, hazards in the surroundings (both man-made and natural), hazards at the site, and business interruption handling capabilities. A break-down of these factors from Ericsson's risk management evaluation tool are provided in Figure 1.

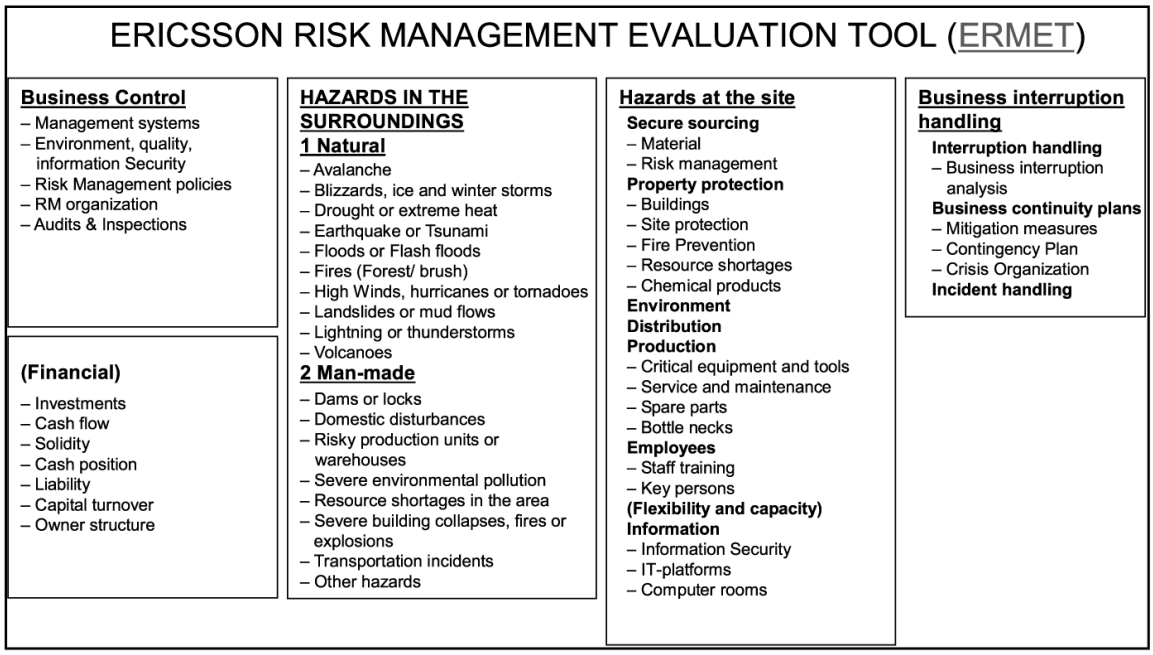


Figure 1 – Factors in Ericsson's Risk Management Evaluation Tool (Norrman and Jansson, 2004)

Additionally, in the risk assessment phase, Ericsson prioritizes risks based on potential financial impact and probability of the risk event occurring (Norrman and Jansson, 2004). This calculation is referred to as a "business interruption value (BIV)" and is an estimate using Equation 1.

$$BIV = (\ Gross\ Margin \times Business\ Recovery\ Time) + Extra\ Costs$$

Equation 1 - Business Interruption Value Equation

In the equation, extra costs include costs such as idle capacity, inventory carrying costs, lost customer confidence, and other cost components (Norrman and Jansson, 2004:446). Risk events are then prioritized for management attention based on their BIV.

To facilitate its risk assessment processes, Ericsson requires its suppliers to maintain secure sourcing and business continuity plans indicating their key suppliers and their risk management strategies and to share these plans with Ericsson (Norrman and Jansson, 2004). Additionally, Ericsson requires its suppliers to place similar requirements on their suppliers and sub-suppliers. These planning and reporting requirements provide Ericsson visibility beyond its first tier suppliers and assist the firm's risk assessment processes.

As part of the risk assessment process, Giunipero and Eltantawy (2004) recommend that risk managers prioritize risks based on four dimensions: 1) degree of product technology involved in the item purchased (high-tech vs. low-tech products); 2) need for security in handling, packaging and transporting the product; 3) importance of the supplier (critical vs. non-critical); and 4) purchasers' prior experience with the situation whether it is a new item, new supplier, or both (limited vs. significant experience). High technology products are riskier than low technology because of the difficulty in evaluating supplier performance and predicting quality and production issues before delivery of the product occurs. Security risks are particularly important to the defense industry because of the potential for theft of technology or tampering/sabotage by foreign governments or non-state actors such as criminal or terrorist groups. Evaluating the importance of a component and the criticality of a supplier is a vital part

of analyzing and prioritizing risks because many components may be produced by only one supplier or a limited number of suppliers and the costs and delays of developing alternative sources may be very high. Finally, when assessing the risk a supplier poses, the focal firm's previous experience or lack of experience with a given supplier is a key factor for consideration. Suppliers with long track records of good performance should be less risky sources of supply then suppliers with a poor record or new suppliers. However, a supplier's circumstances may have changed since previous purchases or the component being supplied may be outside the supplier's normal business area. Analyzing these factors can provide useful insight on the potential risks of sourcing a component from a given supplier (Giunipero and Eltantawy, 2004).

Zsidisin, Panelli, and Upton (2000) assert that a key problem with effectively assessing and prioritizing risk is determining the probability a given risk event might occur. These authors recommend that the total cost of a given risk event must be determined and used in conjunction with a general estimate of the probability of an event occurring to determine the likely cost of a given risk event. One approach to calculating the likely cost of a risk event is to multiply an estimate of the total cost of the risk event by the estimated probability of the event. By calculating the likely cost of each analyzed risk event, risk analysts have a common metric to assist with prioritizing risks.

Additionally, as traditional risk management deals only with identified risks, it is insufficient to ensure supply chain resilience alone (Pettit, Fiksel, and Croxton, 2010). These authors recommend that firms must complement their risk management strategies by improving the firm's other resilience-related capabilities such as flexibility, visibility, and recoverability (Pettit, 2008).

Supply Chain Mapping

Supply chain maps are invaluable tools in risk analysis. Maps provide planners a picture of the supply chain's nodes and the links between those nodes. Additionally, contextual information, such as information regarding the environment in which a link or node operates, can be presented in a supply chain map to quickly allow an analyst to understand the internal and external linkages which influence the supply chain and potentially lead to vulnerabilities and risks (Gardner and Cooper, 2003). Gardner and Cooper (2003) suggest that supply chain maps can be used to aid understanding of the supply chain and alert planners to potential constraints or vulnerabilities in the supply system. Additionally, these authors assert that maps can guide supply chain management and modification efforts (Cooper and Gardner, 2005). Maps can depict not only the flow of goods and services that add value to the customer, but also track the flow of information in the supply chain and highlight the relationships between the links and nodes in the system (Gardner and Cooper, 2003). An example map is provided in Figure 2.

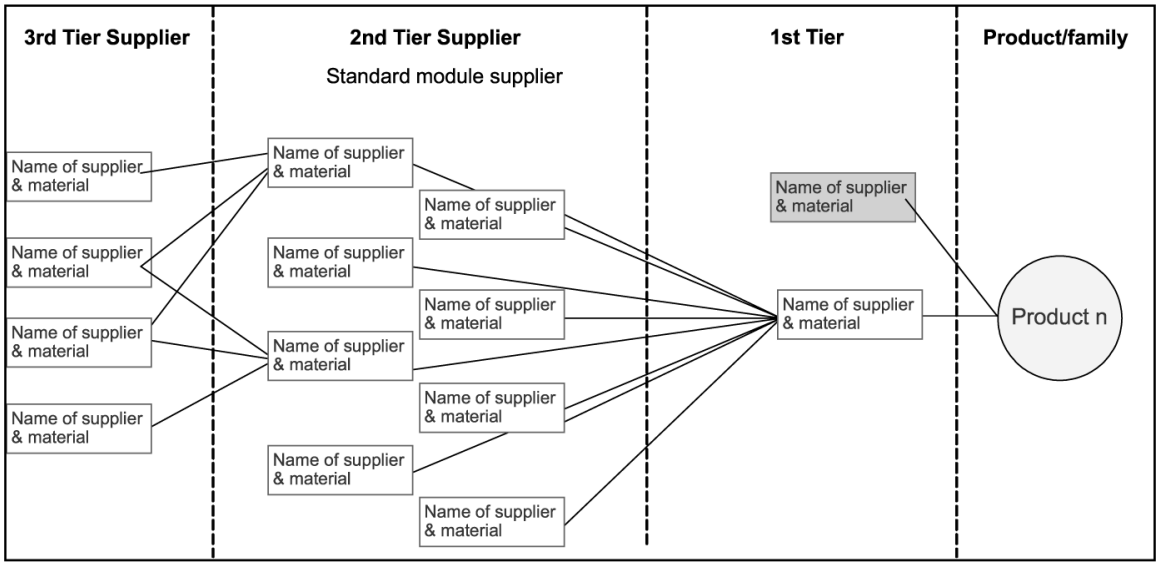


Figure 2 - Example Supply Chain Map (Norrman and Jansson, 2004)

Supply chain maps vary by product or service and process. For example, an electronics firm producing two products will probably have different manufacturing flow processes for each product. Each manufacturing flow process consists of different suppliers and customers. Similarly, each product may have a different order fulfillment process to meet specific customer requirements (Gardner and Cooper, 2003). Given the exponential degree of complexity which may arise during supply chain mapping, it is imperative that managers simplify their maps to the greatest degree possible. While it may appear ideal to list all customers and suppliers from raw materials through end customer, this is often not practical (Gardner and Cooper, 2003).

Generally, when developing a map, it is useful to approach the mapping process as a cartographer (Gardner and Cooper, 2003). In mapping the United States, for example, a cartographer will draw a large-scale map of the entire United States with limited detail and multiple smaller-scale maps of various areas to provide a more detailed representation of the specific features of areas. Additionally, the cartographer will limit the amount of data provided on a map based on the map's intended purpose. In this way, the cartographer makes the map more user-friendly to readers and speeds their ability to rapidly interpret the map and make decisions based on its information (Farris, 2010; Gardner and Cooper, 2003). Likewise, when mapping a supply chain process, maps should only provide data relevant to that process and to the level of detail appropriate for the map's intended use (e.g. senior-executive strategic decision making regarding the process) (Cooper and Gardner, 2005). If users require information from more than one process to make a decision, they should refer to the maps of the relevant processes (Farris, 2010; Gardner and Cooper, 2003). Therefore, a strategic-level map of a given process for a certain product or service should only identify components and relationships that are of

strategic value to the focal firm. For operational level decisions, managers can generate more detailed maps of specific portions of each supply chain process for each product and service as required. To identify touch points between the supply chains processes for each product and service, managers can overlay maps upon one another to highlight intersections and identify opportunities and risks (Farris, 2010).

Difficulty Mapping Supply Chains and Identifying Risks

A review of the supply chain literature consistently highlights the difficulty of comprehensively mapping a given firm's supply chains. In their study of supply chains in the aerospace industry, Haywood and Peck (2004) found that because of the length and complexity of supply chains, it is impractical for a focal firm to single-handedly map and analyze the supply chains of a given aerospace product. To overcome this issue of visibility, some firms require their suppliers to develop and maintain secure sourcing plans and contingency plans with identified back-up sites/resources and share these plans with the firm (Norrman and Jansson, 2004; Zsidisin, Panelli, and Upton, 2000). However, this approach may not be feasible in all cases. Alternatively, Haywood and Peck (2004) suggest that focal firms should focus their efforts on managing risks in the supply chain to their immediate suppliers and customers and rely on the other firms within the supply chain to identify and manage risks to their portions of the supply chain. While this approach does reduce the resources involved in a given firm's supply chain risk management efforts, it potentially leaves the firm exposed to greater risk by not ensuring rigorous risk management across the supply chain.

Application of Private Sector Supply Chain Management Principles to the Defense Industry

Additionally, organizations and supply chains in the defense industry operate in a different environment than those in the larger private sector. The distinctive features of the public sector supply chain organizations include: large and specific services; remote customers; stakeholders are complex, difficult to integrate and crucial to success; dedicated market suppliers; reduced availability of alternatives; accountability to national interest instead of to shareholders; the government makes the rules and can sanction anti-competitiveness; investment cycles are long in comparison to annual reports and returns on investment; and politics drives demand (Humphries and Wilding, 2004). Humphries and Wilding (2004) found that, in general, managers in public sector-driven industries such as defense and managers in the larger private sector are similarly motivated to improve supply chain performance; however, some of the distinctive features of public sector supply chains hampered these efforts. Specifically, problems such as limited trust between customers and suppliers, old products, obsolescence, staff and organizational upheavals, poor end-customer visibility and lack of investment in modern procedures and systems increased the difficulty of supply chain management efforts (Humphries and Wilding, 2004). Despite these distinctive features and their effects on supply chain management, Humphreys and Wilding (2004) suggest the principles which apply to management of supply chains in purely private sector markets also generally apply to public sector supply chains such as those found in the defense industry.

Current DoD and USAF Supply Chain Risk Analysis Processes

To understand supply chain risk management processes in the DoD and the USAF, an in-depth review of applicable policy and guidance regarding risk management in acquisitions programs in these organizations was conducted. The overarching DoD acquisition policy document, Department of Defense Directive (DODD) 5000.01, "The Defense Acquisition System", does not discuss supply chain risk or supply chain resiliency (Department of Defense, 2007). However, DODD 5000.02, "Operation of the Defense Acquisition System", does direct acquisition program managers to ensure programs are cost-effectively sustained throughout their life cycle and directs systems engineers to consider technology and manufacturing risks when designing a system (Department of Defense, 2008). However, the discussion of technology and manufacturing risk in DODD 5000.02 is directed at ensuring programs are developed on time and function as intended, not on whether or not the manufacturing capabilities necessary to sustain the system will be available and secure throughout its life cycle.

Both documents emphasize that defense acquisition programs are performance and cost driven. Neither document addresses the need to ensure resilient supply chains.

However, the Defense Acquisition Guidebook (DAG) does discuss risk management and addresses intelligence support to some risk management processes (Defense Acquisition University, 2012). In the DAG, risk management is divided into two categories: 1) risk management in program protection, and 2) risk management in systems engineering. Risk management in program protection focuses on risks of technology transfer to foreign states and firms. This section provides detailed guidance regarding intelligence and counterintelligence support to program protection and the contributions of these functions to the program protection

plan (PPP). The PPP is the capstone product of the program protection risk management process and outlines the threats to the program and directs actions program participants must take to mitigate these threats and avoid unauthorized technology transfer to foreign competitors (Undersecretary of Defense for Acquisitions, Technology, and Logistics, 2011). Air Force Instruction 14-111, "Intelligence in Force Modernization", provides policy on how intelligence supports program protection for USAF acquisition programs (Department of the Air Force, 2005).

With regards to risk in systems engineering, program managers are directed to manage potential sources of risk to program cost, schedule and performance throughout the program's life cycle. The DAG describes risk as:

> "a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints. Risk can be associated with all aspects of a program (e.g., threat environment, hardware, software, human interface, technology maturity, supplier capability, design maturation, performance against plan,)…"(Defense Acquisition University, 2012: 184).

Specifically, the DAG highlights the need to manage risks in four categories: 1) the technologies being used and their relationship to system design, 2) manufacturing capabilities, 3) potential industry sources for components, and 4) test and support processes (Defense Acquisition University, 2012). To manage these risks, the guide provides a risk management process consisting of five steps: 1) risk identification, 2) risk analysis, 3) risk mitigation planning, 4) risk mitigation plan implementation, and 5) risk tracking (see Figure 3 - DoD Risk Management Process).

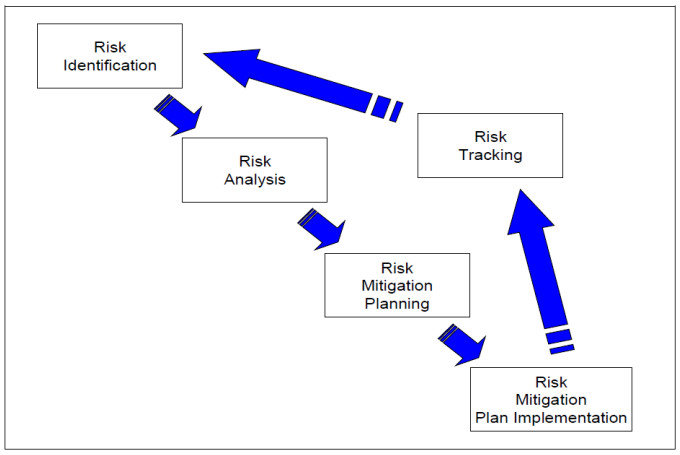


Figure 3 - DoD Risk Management Process (Department of Defense, 2006:4)

The handbook, Risk Management for DoD Acquisition, expands on the guidance provided regarding risk management in the DAG (Department of Defense, 2006). While the handbook focuses on program protection, it does provide guidance regarding risk management in systems engineering. Specifically, the guide provides a detailed methodology using the same five-step risk management process outlined in the DAG. However, the handbook focuses on providing program managers and other acquisition team members with an understanding of risk management practices, but does not provide specific tools to assist risk management.

Similar to academic descriptions of the concept of risk, the handbook asserts risk has three components (Department of Defense, 2006:1):

"1. A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,

2. A probability (or likelihood) assessed at the present time of that future root cause occurring, and

3. The consequence (or effect) of that future occurrence."

Additionally, the handbook identifies 16 risk sources: threats, requirements, technical baseline, test and evaluation, modeling and simulation, technology, logistics, production/facilities, concurrency, industrial capabilities, cost, management, schedule, external factors, budget, and earned value management system. The discussion of most of these terms is outside the scope of this paper; however, the following three are relevant to the discussion of supply chain risk management:

1. Logistics. The ability of the system configuration and associated documentation to achieve the program's logistics objectives based on the system design, maintenance concept, support system design, and availability of support data and resources.
2. Production/Facilities. The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources (repair resources in the sustainment phase).
3. Industrial Capabilities. The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system. (Department of Defense, 2006)

The handbook covers all five steps of the risk management process in detail; however, for the purposes of this paper, we will focus on the risk identification and risk analysis steps. With regards to risk identification, the handbook advises managers to follow the process below (Department of Defense, 2006):

1. List work breakdown structure product or process elements,
2. Examine each in terms of risk sources or areas,

3. Determine what could go wrong, and
4. Ask "why" multiple times until the source(s) is discovered.

To facilitate risk identification, the handbook advises that "risks can be identified based on prior experience, brainstorming, lessons learned from similar programs, and guidance contained in the program office [risk management plan]" (Department of Defense, 2006:7). Additionally, the handbook recommends the use of a cross-functional team to identify risks.

With regard to risk analysis, the intent of this step of the risk management process is to determine "how big the risk is" (Department of Defense, 2006:11). The handbook directs managers to:

1. Consider the likelihood of the root cause occurrence and assign the risk a likelihood level according to the guidance provided in the Table 4.

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~30%
3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

Table 4 – Levels of Likelihood Criteria (Department of Defense, 2006:12)

2. Identify the possible consequences in terms of performance, schedule, and cost and assign the risk a consequence level using the guidance provided in Table 5.

Level	Technical Performance	Schedule	Cost
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	Able to meet key dates. **Slip < * month(s)**	Budget increase or unit production cost increases. **< ** (1% of Budget)**
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float. **Slip < * month(s)** **Sub-system slip > * month(s) plus available float.**	Budget increase or unit production cost increase **< ** (5% of Budget)**
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected. **Slip < * months**	Budget increase or unit production cost increase **< ** (10% of Budget)**
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones. **Slip > * months**	Exceeds APB threshold **> ** (10% of Budget)**

Table 5 – Consequence Levels (Department of Defense, 2006:13)

3. Identify the risk level using the Risk Reporting Matrix shown in **Error! Reference source not found.**.

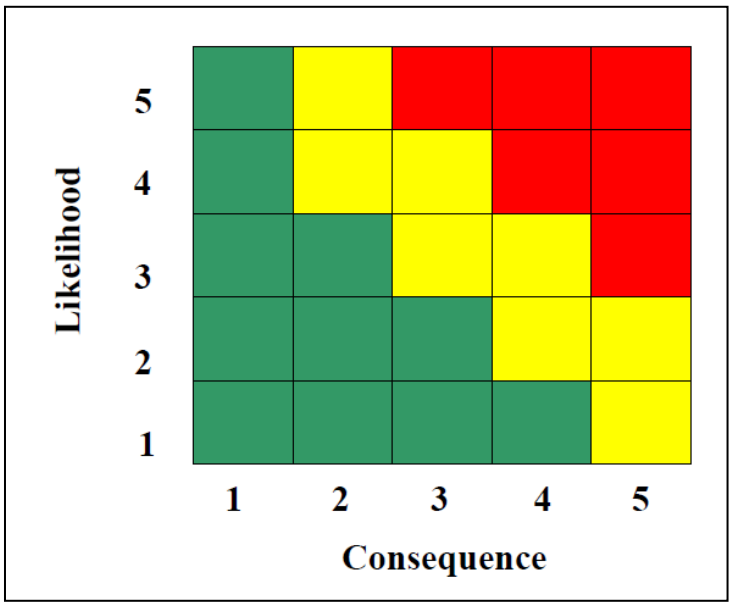


Figure 4 - DoD Risk Reporting Matrix (Department of Defense, 2006:11)

Using this process, managers can properly prioritize identified risks for mitigation planning and actions. Consistent with other DoD acquisitions guidance, the discussion of risk analysis in the handbook focuses on ensuring programs are developed and operationally fielded on time and within budget; however, the guidance does not address the issue of ensuring supply chain resiliency once a program is fielded or intelligence support to risk assessment (Department of Defense, 2006).

Intelligence Support to Acquisitions

AFPD 14-1, "Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources and Operations", the over-arching policy document for USAF intelligence directs embedding "intelligence into Air Force acquisition programs to ensure early and sustained support throughout the life of a program" (Department of the Air Force, 2004:2). Furthermore,

USAF intelligence analysts are directed to use the Predictive Battlespace Awareness (PBA) process in order to understand the operational environment, adversary capabilities, and predict adversary courses of action (COAs). By performing PBA, intelligence analysts can provide commanders the capability to anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions (Department of the Air Force, 2008).

The PBA process is comprised of five sub-functions: 1) Intelligence Preparation of the Operational Environment (IPOE), 2) Target Development, 3) ISR Strategy and Planning, 4) ISR Operations, and 5) Assessment (Department of the Air Force, 2008). Of these five functions, IPOE is the one most closely aligned with the concept of risk assessment. According to AFI 14-124, IPOE is described as:

> "[t]he systematic, four-step analytical methodology employed to reduce uncertainties concerning the adversary and to allow friendly forces to exploit or minimize the undesirable effects of the Operational Environment. The four steps of IPOE are: Define the Operational Environment; Describe the Operational Environment's Effects; Evaluate the Adversary; and Determine the Adversary's Course of Action" (Department of the Air Force, 2008:9).

The IPOE process is detailed in Air Force Pamphlet (AFPAM) 14-118, "Predictive Battlespace Awareness: Air and Space Intelligence Preparation of the Operational Environment" (Department of the Air Force, 2008). Through the IPOE process, intelligence analysts identify potential risk events, their impacts, and determine their likelihood. USAF IPOE guidance is directed toward providing intelligence support to operations planning and execution. AFPAM 14-118 does not address the application of the IPOE process to other areas such as intelligence support to acquisition; however, the pamphlet asserts the process is applicable to all mission types (Department of the Air Force, 2008).

Conclusion

DoD risk management guidance generally follows the current theories and concepts identified and described in risk management academic literature. However, while current acquisitions policy does address broad risk management in detail, little attention is paid to the specific problem of managing supply chain risk and ensuring resiliency during program sustainment. In particular, the available guidance regarding intelligence support to acquisitions programs only addresses protection against unauthorized or unintentional compromise of technologies to foreign firms or powers (Department of Defense, 1994; Department of Defense, 2008; Department of Defense, 2010; Defense Acquisition University, 2012; Department of the Air Force, 2005). Based on this literature review, there appears to be a gap in DoD acquisitions and intelligence policy and guidance regarding supply chain risk management in general and intelligence support to supply chain risk management in particular. The remainder of this paper is intended to help fill this gap by providing a methodology for intelligence analysts to use to provide intelligence support to supply chain risk management using the established IPOE process.

IV. Intelligence Support to Supply Chain Risk Management

Overview

Effective intelligence support to supply chain risk management allows commanders, program managers and other acquisitions decision-makers to better understand their supply chains, the environments in which those supply chains operate, and the risks/threats to their supply chains. Armed with this information, managers can make informed decisions regarding their supply chain operations considering not only cost and performance, but also resilience. This paper will provide a methodology based on the IPOE process outlined in JP 2.1-3 and AFPAM 14-118 to enable intelligence analysts to provide timely, accurate, predictive and usable intelligence to acquisitions leaders to drive supply chain planning and execution decisions (Department of the Air Force, 2008; Joint Chiefs of Staff, 2009). The methodology outlined in this paper will focus on differences in conducting IPOE in support of supply chain risk management versus other military operations.

As discussed previously, the IPOE process has four steps with each step consisting of multiple sub-steps. The following sections will discuss the application of the IPOE process to the problem of providing intelligence support to supply chain risk management.

Step 1: Define the Operational Environment

The purpose of this step is to define the limits of the operational environment to and establish the boundaries of the intelligence problem (Department of the Air Force, 2008). In this context the operational environment is the set of external factors which are likely to influence the

supply chain. The operational environment includes not only the physical environment (e.g. weather, climate, geography, etc.), but also non-physical factors such as politics, culture, information and military influences (Joint Chiefs of Staff, 2009). Step 1 identifies the characteristics of the operational environment and highlights the factors which might impact the supply chain. Step 1 consists of seven sub-steps (Joint Chiefs of Staff, 2009):

1. Identify the force's operational area;
2. Analyze the mission and joint force commander's intent;
3. Determine the significant characteristics of the operational environment;
4. Establish the limits of the joint force's areas of interest;
5. Determine the level of detail required and feasible within the time available;
6. Determine intelligence and information gaps, shortfalls, and priorities; and,
7. Collect material and submit requests for information to support further analysis.

1.1. Identify the Force's Operational Area

In this sub-step, the boundaries of operations are identified. In the context of supply chain risk analysis, these boundaries are the boundaries of the supply chain itself. Determining the boundaries of a given weapon system supply chain is typically not an easy task. From an academic perspective, this is best done through a complete supply chain map of the supported weapon system. However, for reasons discussed in the following paragraphs this may not be feasible. To overcome this difficulty, we explore two approaches to this problem: 1) a complete supply chain map and 2) a focused approach.

1) Complete supply chain map:

The most effective way to determine the boundaries of the supply chain for a weapon system is to identify the components and sub-components which comprise the weapon system and then separately map the supply chain for each of the components and sub-components from the finished product back to the source of the raw materials which are used in the product. If the weapon system contains any reparable items, the supply chain map for each product must also identify the repair pipeline for that product.

In this context, a supply chain map requires a significant amount of contextual data to be useful. First, the map must now not only identify the firm which contributes a given part, piece of hardware and/or software, or raw material to the supply chain, but also identify the location of the factory, mine, or other facility which provides the resource, the ownership of the facility, the degree of foreign ownership or involvement in the firm and/or facility (e.g. Chinese private firms are typically partially state-owned or the state has significant influence on the operations of the firm and/or facility), and, for foreign facilities, the citizenship and demographics of the workers and managers. Additionally, the map must provide similar detail of the logistics chain (e.g. ships, ports, rail facilities, warehouses, etc.) which transports and stores the resource along the supply chain path as products are vulnerable to theft and/or tampering during these steps as well.

To collect the necessary information to develop a supply chain map, analysts must rely on the weapon system's program management office as their key source of information. Through the program manager, analysts can collect the necessary information to identify the firms, facilities, and the logistics network that comprises links and nodes of the supply chain by soliciting information from the prime contractor and their suppliers. With this baseline

information in hand, analysts can begin to collect the information necessary to fill-in the contextual information of the supply chain map as discussed in the preceding paragraph. Geospatial software such as FalconView can be used to organize the supply chain map and contextual information into layers which can be overlaid onto maps, charts, and/or imagery to simplify analysis.

While this approach may seem ideal because it results in a complete map of the supply chain for each component and sub-component within the weapon system, it has several drawbacks. First, it is generally not feasible due to the complexity of most supply chains and the lack of sufficient analytical time to map the entire chain. For example, the F-22 is comprised of several thousand individual parts and has a supply chain consisting of approximately 1,100 sub-contractors (Hennigan, 2011). Even a device as small as cell phone contains several hundred parts potentially sourced from over a hundred manufacturers. Additionally, in many cases, without extensive investigative research, it is difficult to map most supply chains beyond the first and possible second tier suppliers of the prime contractor. This difficulty is due to two key factors. First, the prime contractor and first tier suppliers are generally the most visible players in the supply chain and the prime contractor rarely has information on where his first tier suppliers source their components because this is proprietary information. Second, as the prime contractor and their suppliers continuously seek the lowest cost and most reliable sources for their parts, the supply chain is continually changing. This change is especially apparent for parts that are commodities (e.g. steel, memory chips, some electronic components, etc.) and for certain logistics services (e.g. transportation, warehousing, etc.). As a result of these factors, some elements of the supply chain map can never be fully detailed as they are in almost constant flux.

2) Focused Approach

Given the inherent difficulties on making a complete map of a weapon system's supply chain, it may be preferable not to attempt to map the supply chain in its entirety in detail, but to focus analytical efforts on likely sources of risk. Using this technique, a broad overview of the weapon system supply chain map will be created allowing analysts and decision-makers to see the big picture of the supply chain's operations and its operating environment. Additionally, analysts will map risky areas of the supply chain in detail to allow focused evaluation of these portions of the supply chain and the threats to their operations.

One way to accomplish this focused approach is through the use of a cross-functional working group of subject matter experts. This working group should be charged with identifying the components and/or sub-components they believe are most vulnerable to deliberate disruption by an adversary. To assist the process of nominating high risk components, the working group should use Levels 2 and 4 of Peck's drivers of supply chain vulnerability framework as discussed in the literature review (Peck, 2005a). Using this framework, in Level 2, the supply chain should be considered "in terms of the assets and infrastructure needed to produce and carry the goods and information flows", the vulnerability of the network in terms of the probabilities and impacts of the "loss of links, nodes, and other essential operating assets" (Peck, 2005a:219). Additionally, in Level 4, the "wider macroeconomic and natural environment" in which the supply chain and its nodes and links exist should be considered (Peck, 2005a:223). The potential impacts of man-made forces such as political, economic, social, and technological forces as well as natural forces such as geology, ecology, pathology, and weather should be identified and analyzed (Peck, 2005b). Finally, the group must consider unique technologies, limited

availability raw materials or manufacturing capabilities, and components with either a single supplier or limited numbers of suppliers as potential targets for adversary actions. A flow chart of the focused approach process is provided in Figure 5.

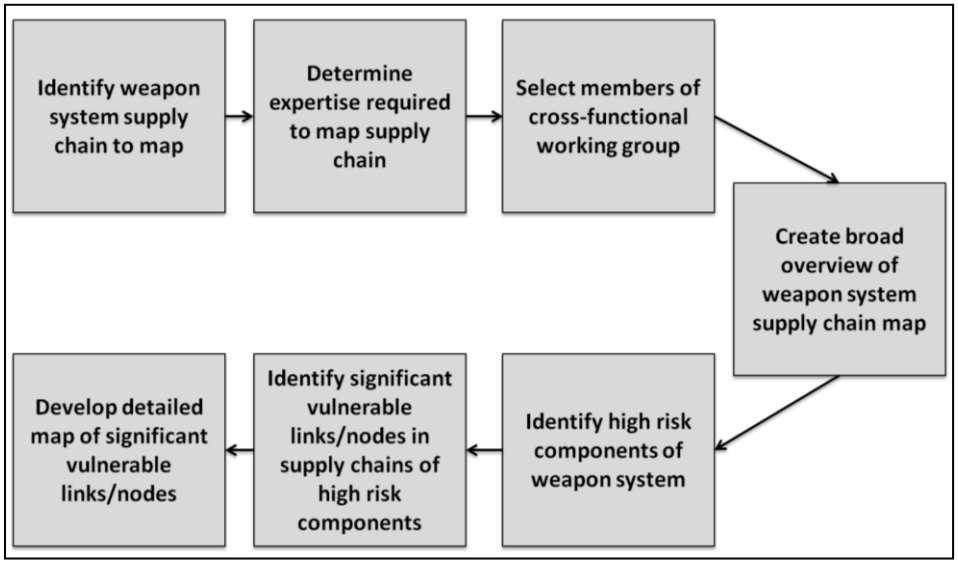


Figure 5 - Focused Approach Process Flow Chart

Given these considerations, in a brainstorming session, each member of the working group should nominate components or sub-components they believe may be vulnerable to disruption or tampering by an adversary state or non-state actor and state the risk events they believe have vulnerable components.

To effectively consider the potential sources of supply chain threats without mapping the supply chain in detail requires a high level of expertise regarding the links and nodes of the supply chain and the environment they operate within. At a minimum, the working group that conducts this analysis should consist of contracting and logistics professionals from the prime contractor and their first tier suppliers, intelligence analysts, counterintelligence analysts, and logistics and acquisitions experts from the program management office. If second and/or third

tier supplier representatives are available, these individuals should also participate in the working group.

While this approach has the benefit of being much more efficient than the complete supply chain map approach, it has the inherent drawback of being less comprehensive. As a result, while this approach should identify many, if not most, of the threats to the supply chain, it is likely some threats will not be identified potentially allowing an adversary the opportunity to exploit a unidentified supply chain vulnerability.

1.2. Analyze the Mission

In this sub-step, analysts define the intelligence problem based on the mission. A properly defined intelligence problem focuses the IPOE effort ensuring the relevant aspects of the operational environment are analyzed while minimizing effort wasted analyzing irrelevant characteristics. When providing intelligence support to supply chain risk management, the overall mission is to provide a secure and resilient weapon system supply chain. In support of this overall mission, the intelligence mission is to identify potential threats to the supply chain, characterize those threats, and predict potential adversary COAs which threaten the supply chain.

1.3. Determine the Significant Characteristics of the Operational Environment

Given the operational area and mission identified in sub-steps 1 and 2, analysts must determine the specific areas on which to focus intelligence collection and analysis efforts. Using the supply chain map and/or risk events identified in sub-step 1, analysts must prioritize areas for attention based on their likelihood and potential impact on the weapon system supply chain.

This prioritization should be cursory and does not need to be exact. The final product of this sub-step is a prioritized list of identified characteristics of the environment and potential threats which might impact the supply chain.

To aid the prioritization effort and identify the significant characteristics of the operational environment in order to focus intelligence efforts requires significant expertise regarding the supply chain and potential threats to the supply chain. To provide this expertise, it is recommended that a cross-functional working group, similar to that discussed in sub-step 2, is employed to conduct this analysis. The working group must consider the environment within which each supply chain link and node resides from both a physical and non-physical perspective. For example, if a part or raw material is sourced from a foreign nation, analysts must consider the political, military, cultural, and economic characteristics of that nation and determine if an adversary state or non-state actor has the capability and intent to disrupt or tamper with the manufacturing and/or logistics operations which provide that part or material to the supply chain.

1.4 Establishing the Limits of the Force's Area of Interest

Per JP 2-01.3, the "operational environment encompasses all characteristics, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission" (Joint Chiefs of Staff, 2009:II-5). This definition can be applied directly to the problem of protecting a weapon system supply chain. Additionally, while the operational environment is vast, the area which is relevant to intelligence responsibilities is more limited. With regards to manufacturing and logistics, determining the capabilities of these firms to

effectively perform their functions in the supply chain is not an intelligence function. Instead, the IPOE effort should be directed at identifying and assessing threats to the supply chain due to foreign state actors and/or non-state actors such as foreign intelligence agents, insurgent groups, criminals, and/or terrorists.

For example, while the supply chain will include both foreign and domestic manufacturing and logistics firms, the capabilities and financial condition of these firms is outside the responsibility of military intelligence. However, the supply chain may be threatened by deliberate disruption or tampering by criminals, terrorists, or foreign agents and protecting the supply chain against these threats falls under the responsibilities of intelligence, counterintelligence and law enforcement depending upon the nature of the threat (e.g. foreign state versus domestic non-state actor, non-state actor versus criminal group).

As a result, in the context of supply chain risk analysis, the area of interest should be defined as the portion or characteristics of the operational environment which may affect current and future supply chain operations (Joint Chiefs of Staff, 2009). Intelligence support to risk analysis must focus on identifying, monitoring and predicting "adversary, neutral, or other activities" within the operational environment and supply chain which may impact current or future supply chain operations (Joint Chiefs of Staff, 2009:II-6). In this context, the area of interest does not only include the host country or geographic area of a manufacturing firm, logistics firm, or transportation lane, but also neighboring countries and other areas which have the capabilities and/or intentions to threaten the supply chain. At its broadest extent, the area of interest may include areas that are far away from the supply chain's links and nodes

geographically, but through cyberspace or other domains and means have the potential to affect the supply chain's operations.

1.5. Determine the Level of Detail Required and Feasible Within the Time Available

As in all operations, scarce resources dictate a balance be struck between effectiveness and efficiency. To that end, analysts must determine the appropriate amount of detail required and achievable to effectively identify and assess threats to the supply chain. The level of detail and attention allocated to each identified risk should be commensurate with that risk's priority as determined in sub-step 3 based on the relevant threat's capability to disrupt the supply chain and its ability to do so.

1.6. Determine Intelligence and Information Gaps, Shortfalls, and Priorities

As in IPOE for other military operations, identifying prioritized intelligence requirements (PIR) and information gaps and shortfalls is a critical step to ensuring the necessary intelligence is available for successful threat identification and analysis. Analysts should use the prioritized list of identified characteristics of the environment and potential threats developed in sub-step 3 as the basis for developing PIRs. Once PIRs are developed, analysts should conduct preliminary research to identify intelligence gaps and shortfalls for collection.

1.7. Collect Material and Submit Requests for Information to Support Further Analysis

While the process of collecting material remains the same, it is important to realize that much of the necessary information for intelligence support to risk analysis will need to be

gleaned from sources outside typical military intelligence channels. As a result, analysts will need to collect information from and submit requests for information to agencies outside the DoD. For example, to obtain information regarding the firms, facilities, and services which form the physical structure of the supply chain, intelligence analysts will need to collaborate with the relevant weapon system program manager, the prime contractor, and potentially, the prime contractor's suppliers. Similarly, intelligence regarding individual foreign firms, foreign intelligence organizations, and non-state actors will need to be gathered from non-military intelligence sources such as the Central Intelligence Agency, Federal Bureau of Investigations, the Department of Homeland Security, and other military and non-military counter-intelligence and law enforcement agencies. It is important for organizations and analysts responsible for intelligence support to supply chain risk management to establish habitual relationships with the agencies and learn to utilize those agencies processes and resources to collect the necessary intelligence and submit requests for information to conduct their analysis.

Step 2: Describe the Operational Environment's Effects

Per AFPAM 14-118, "[t]he operational environment imposes constraints and provides opportunities to adversary and friendly forces that are crucial in predicting potential adversary COAs and developing friendly COAs" (Department of the Air Force, 2008:13). The purpose of this step is to determine how the characteristics of the environment influence the supply chain and provide opportunities to adversary and friendly forces. Through analysis of the environment's effects on the supply chain and the adversary's ability to affect the supply chain,

analysts can better predict adversary COAs and identify friendly opportunities to improve supply chain resiliency. This step has three sub-steps (Joint Chiefs of Staff, 2009):

1. Develop a geospatial perspective of the operational environment
2. Develop a systems perspective of the operational environment
3. Describe the impact of the operational environment on adversary and friendly capabilities and broad COAs

2.1. Develop a Geospatial Perspective of the Operational Environment

Developing a geospatial perspective of the operational environment helps analysts identify the relevant physical, non-physical, and locational aspects of operational environment (Joint Chiefs of Staff, 2009). In this sub-step, each aspect of the operational environment identified in step 1 is evaluated to determine its relevance to the supply chain's operations and, if relevant, to identify its potential impact on the supply chain.

To assist the process of determining operational environment effects on the supply chain, analysts should overlay the supply chain maps for critical weapon system components over a geographic map of the relevant portion of the earth's surface. The scale of this map should be large (e.g. 1:5,000,000 or larger) to allow all of the key links and nodes to be depicted on the map. Ideally, the supply chain map should be created as an electronic graphical overlay to allow it to be overlaid over electronic maps of various scales as needed for analysis. Additional contextual information such as country borders, crime information, terrorist organization operating areas, etc. should be created in separate overlays as applicable to allow this information to be easily manipulated and evaluated graphically by analysts in the context of the

larger supply chain and operational environment. The evaluation of the operational environment should be at the operational level to maintain analytical focus and avoid being bogged down in relatively inconsequential details.

With a geographic representation of the critical links and nodes of the supply chain in hand, analysts should consider the impacts of the physical environment on the supply chain. To support this analysis, analysts should graphically depict the characteristic of the environment which might impact the supply chain. Specifically, analysts must consider:

1. Terrain effects,
2. Weather effects (e.g. 2011 tsunami impact on Japanese manufacturers),
3. Political effects (e.g. Chinese control of 95% of global rare earth element production) (Bell, 2012),
4. Infrastructure (e.g. air and sea port facilities, rail and roadways, warehouses)
5. Air and sea lines of communication (e.g. piracy threat),
6. Information networks (e.g. unintended access to sensitive information passed over unsecure foreign-controlled networks),
7. Cultural and religious effects (e.g. a facility may be staffed by workers who are generally hostile to the U.S. for cultural or religious reasons),
8. Economic effects
9. Military effects (e.g. potential disruption of supply chain by adversary or neutral military actions), and
10. Other effects (e.g. sabotage of hardware or software by foreign intelligence or military agents) (Joint Chiefs of Staff, 2009).

The above list is not intended to be exhaustive, but should provide a starting point for consideration of potential effects of the operational environment. Because of the uniqueness of the each supply chain and its operational area, analysts should carefully identify the characteristics of their tasked operational area and consider their potential impacts on a given supply chain (Joint Chiefs of Staff, 2009).

2.2. Developing a Systems Perspective of the Operational Environment

To facilitate analysis of how the characteristics of the operational environment may impact the supply chain, it is useful to view the characteristics and their effects as a system of systems. For example, instead of evaluating how an adversary's political, economic, and military systems may impact the supply chain independently, analysts must consider how those systems interact with one another and how those interactions potentially impact or threaten the supply chain (Joint Chiefs of Staff, 2009).

Given the characteristics of the operational environment and the potential effects of those characteristics identified in the preceding steps of the IPOE process, analysts should identify how the separate systems in the environment (e.g. political, economic, military, cultural, religious, social, informational, etc.) influence one another, shape the environment, and potentially effect the supply chain. For example, the host country for a given manufacturing firm which produces a key component in a weapon system supply chain may have a legal environment which does not adequately protect information property and permits the production of counterfeit parts, potentially threatening the flow of reliable parts from this source. This legal environment is caused by the interaction of the country's political, economic, social, and cultural systems.

Chapter II of JP 2-01.3 provides a detailed methodology for analyzing systems and identifying their links and nodes. This level of analysis may be ideal if time and information is available; however, it is probably only necessary for the most significant potential effects on the supply chain. However, analysts should conduct a general analysis of the interactions of the various systems within the environment so that they have an understanding of the forces acting within the operational environment and how those forces interact and affect the supply chain.

2.3. Describing the Impact of the Operational Environment on Adversary and Friendly Capabilities and Broad COAs

Per JP 2-01.3, analysts must combine their findings from the geospatial and systems perspective evaluations into a single integrated assessment which can be easily understood by commanders, operations planners and intelligence professionals (Joint Chiefs of Staff, 2009). To simplify the digestion of this material and aid in the analysis of adversary capabilities and COAs, it is recommended that an individual assessment of the operational environment's impact be given for each significant supply chain node and link identified in step 1 of the IPOE process. To facilitate this analysis, an example product is provided in Table 6.

Critical Radar Component #4 – Node 2: Sichuan Manufacturing Plant (Chengdu, PRC)		
Description: Manufacturers radar sub-assembly component #4		
Characteristic	Description	Effect
Political	Plant is 60% owned by PLAF	1. Production of radar component #4 may be halted/delayed if tensions increase between US and PRC government. 2. PRC government may direct production of faulty components to disrupt US supply chain/operations
Cultural	Workers are 95% Han Chinese and staff is vetted for loyalty by the Communist Party	1. Expect workforce to be loyal to PRC government 2. Difficult to conduct counterintelligence operations within facility
Economic	Plant also manufactures radar components for PLAF fighter aircraft and other customers, including some export customers	Potential exists for technology transfer from radar component #4; however, PRC radar technology is already on level with that used in component
Military	Plant is 60% owned by PLAF	In the event PLAF requires additional radar components due to increase in operations tempo or aircraft production, production of radar component #4 may be halted/delayed
Criminal	Some managers/ workers in plant associated with organized crime group	1. Potential exists for theft of good and/or defective radar component #4 and possible resale to other suppliers 2. Possible introduction of counterfeit goods in radar component #4 supply chain

Table 6 – Example Effects of Operational Environment Analysis of a Hypothetical Supply Chain Node

Step 3. Evaluate the Adversary

Per JP 2-01.3, in this step of the JIPOE process, analysts identify and evaluate the "adversary's capabilities and limitations, current situation, COGs [centers of gravity], and the doctrine, patterns of operation, and TTP [tactics, techniques, and procedures] employed by adversary forces, absent those constraints identified during step two" (Joint Chiefs of Staff, 2009:II-55). Through identifying the adversary's operational capabilities and patterns of behavior and applying this understanding to present and potential future situations, analysts can

determine potential actions an adversary may take to effect the weapon system supply chain given a specific situational context.

In the context of supply chain risk analysis, it is key to evaluate the adversary threat based on the capability to disrupt the supply chain and intent to disrupt the supply chain. Except in a wartime situation or other military conflict, it is unlikely that a potential adversary will exercise overt kinetic and non-kinetic means to attack a weapon system's supply chain. Instead, during typical peacetime operations, potential adversaries will seek to undermine supply chains covertly. As a result, analysts should seek to identify adversary doctrine, training, units or equipment which are potentially targeted at industrial espionage and/or sabotage as well as information operations capabilities such as cyberwarfare. It is unlikely potential adversaries will publicly release information regarding the development of covert operations or capabilities. Similarly, it is important to note that these covert capabilities are unlikely to be maintained in the adversary's conventional military forces. Because of this, it is critical for analysts to look for these capabilities in the adversary's larger government, intelligence, business, and academic systems.

Once adversary capabilities to disrupt a weapon system supply chain are determined, the centers of gravity that enable those capabilities must be identified (Joint Chiefs of Staff, 2009). Understanding centers of gravity that enable the adversary's operations is critical to anticipating adversary COAs. In the context of supply chain risk analysis, an adversary center of gravity may be a capability such as a cyber warfare attack capability, but it may also be an enabler such as access to a manufacturing or storage facility in their country or within one of their ally's borders. To assist in the identification of centers of gravity, analysts should identify the vulnerabilities in

the supply chain which allow the adversary to hold the weapon system at risk. The adversary's abilities to exploit these vulnerabilities are often key centers of gravity which may be vulnerable to attack or denial by friendly forces.

Step 4. Determining Adversary COAs

Given the intelligence collection and analysis conducting in the previous IPOE steps, analysts must assess the adversary's most likely and most dangerous COAs (Department of the Air Force, 2008). These assessments of adversary COAs to disrupt the weapon system supply chain are the final output of the IPOE process. These assessments are critical to effective supply chain risk management because they allow program managers and other decision-makers to make informed decisions about the threats to the supply chain and how to best mitigate those threats. While the final output of the IPOE process will typically be these two potential adversary COAs, it is important to note that each COA may include multiple operations by the adversary. To develop these COAs, JP 2-01.3 provides the following set of sub-steps (Joint Chiefs of Staff, 2009):

1. Identify the adversary's likely objectives and desired end state
2. Identify the full set of adversary COAs
3. Evaluate and prioritize each COA
4. Develop each COA in the amount of detail time allows, and
5. Identify initial collection requirements.

4.1. Identify the Adversary's Likely Objectives and Desired End State

Before determining an adversary's potential COAs to disrupt a weapon system's supply chain, it is imperative to identify the adversary's strategic, operational, and tactical level objectives. These objectives identify the adversary's intent and establish the adversary's likely measures of success. In the context of supply chain risk management, an example of an adversary's operational level goal might be as follows: to covertly reduce the reliability of weapon system X and decrease US force confidence in weapon system X. This example of an adversary objective establishes the adversary's intent with regards to disrupting the weapon system X supply chain (e.g. decrease reliability and confidence in weapon system X) and communicates the level of risk the adversary is willing to accept (e.g. operations against the supply chain must be covert). Using this assessed objective, analysts can evaluate the supply chain, the operational environment, and the adversary's capabilities and doctrine to identify potential adversary COAs.

4.2. Identify the Full Set of Adversary COAs

In this step, analysts generate a list of all potential adversary COAs to disrupt or degrade the weapon system supply chain. This list should include all potential actions which the adversary may take based on their doctrine, capabilities, and/or historical operations and plans. In addition, analysts must not simply list these COAs generally, but must also outline the basic timing and extent of adversary operations under each COA in order to allow the COAs to be compared and evaluated.

To be included in this list, a potential COA must meet the following five criteria: suitability, feasibility, acceptability, uniqueness, and consistency with adversary doctrine or patterns of operation (Joint Chiefs of Staff, 2009). As these criteria are detailed in Chapter II of JP 2-01.3, they will not be discussed in detail in this paper. However, it is important to note that because adversary intentions, plans, and doctrine regarding operations to disrupt US weapon system supply chains will often be intelligence gaps, analysts will need to develop COAs using the best available assessments of these areas. Additionally, analysts must be careful not to limit the list of potential COAs to operations which lie within the bounds of an adversary's known or assessed doctrine and training. If a COA is feasible, acceptable, and suitable, analysts should consider it a valid option for the adversary to pursue (Joint Chiefs of Staff, 2009).

4.3. Evaluating and Prioritizing Each COA

Per JP 2-01.3, once the full list of potential adversary COAs are identified, analysts must evaluate and prioritize them in two lists (Joint Chiefs of Staff, 2009). In the first list, the COAs should be prioritized according to their likelihood. In the second list, the COAs should be prioritized based on the danger they pose to the supply chain's operations. To accomplish this evaluation, analysts should follow the procedures below (adapted from Joint Chiefs of Staff, 2009).

1. Analyze each COA to identify its strengths and weaknesses and the adversary centers of gravity which enable it.
2. Evaluate how well each COA meets the criteria of suitability, feasibility, acceptability, uniqueness, and consistency with adversary doctrine and training. The analyst should

avoid cultural bias and mirror imaging by considering these criteria in the context of the adversary's culture.

3. Evaluate how well each COA takes advantage of the operational environment and the supply chain's vulnerabilities.
4. Compare each COA and determine which one offers the greatest advantages while minimizing risk.
5. Consider the possibility that the adversary may choose the second or third most likely COA while attempting a deception operation portraying adoption of the best COA.
6. Analyze the adversary's current dispositions and recent activity to determine if there are indications that one COA has already been adopted.
7. Guard against being "psychologically conditioned" to accept abnormal levels and types of adversary activity as normal. Identify and focus in greater detail on those adversary preparations not yet completed that are, nevertheless, necessary to accomplish a specific COA.

4.4. Developing Each COA in the Amount of Detail that Time Allows

In this step, each potential COA should be developed in sufficient detail to describe the adversary operations to disrupt the supply chain, the earliest time the operations can begin, where the adversary actions will occur, the adversary's objectives in adopting the COA, and the adversary's desired end state at the end of operations (Joint Chiefs of Staff, 2009). To efficiently allocate intelligence resources, each COA should be developed in priority order based on its likelihood of adoption by the adversary. To facilitate this analysis and graphically depict the

adversary's specific operations under each COA, JP 2-01.3 advocates the use of situation templates and details their creation (Joint Chiefs of Staff, 2009). Although these situation templates were originally intended to depict conventional military operations, they are readily adaptable to operations against weapon system supply chains.

JP 2-01.3 describes situation templates as depictions of adversary forces positions and operations at a "specific time and place relative to an individual COA" (Joint Chiefs of Staff, 2009:II-73). In the context of adversary operations against a weapon system supply chain a situation template should identify the who, what, where, why, and how of the adversary's operations against the supply chain. For example, Figure 6 outlines a hypothetical adversary COA identifying operations to tamper with parts in storage at a port facility, the situation template for this COA should describe these operations, identify which adversary agencies or units are conducting them, approximately when they might be conducted, indicate how the tampering might be accomplished and what the adversary intends to achieve by conducting these operations. By graphically and succinctly providing this information in a situation template of each COA, analysts help program managers and other decision-makers to quickly understand potential adversary operations and develop effective strategies and tactics to either deter, degrade, or defeat these operations.

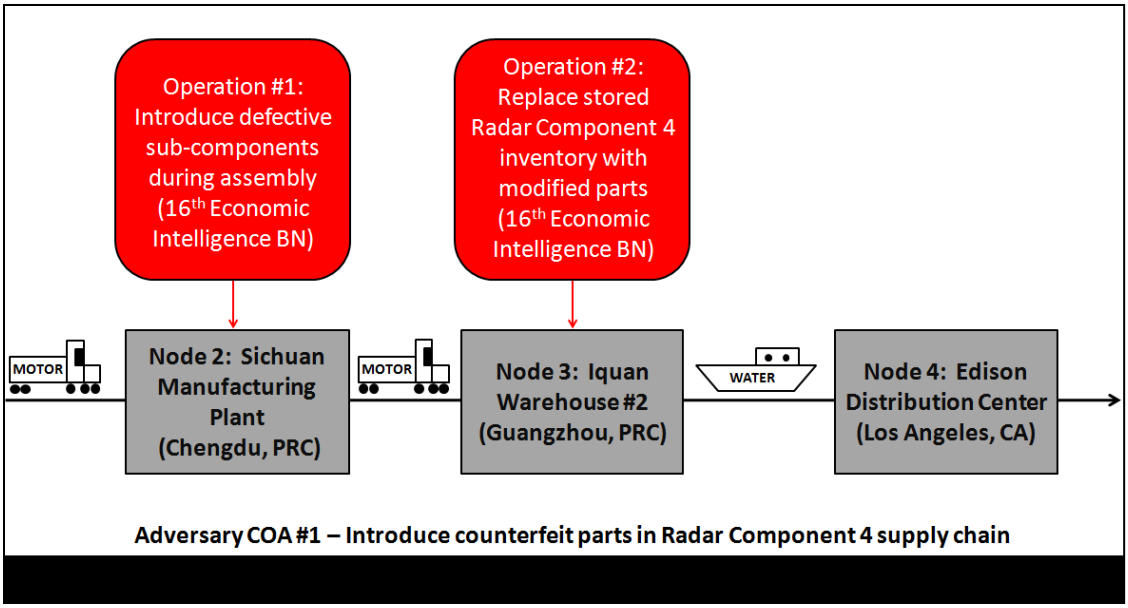


Figure 6 - Example Situation Template

4.5. Identifying Initial Collection Requirements

Based on the assessed most likely and worst case adversary COA, analysts should develop a set of collection requirements to determine which COA the adversary has chosen to execute (Joint Chiefs of Staff, 2009). The collection requirements should be based on observable actions the adversary must take to prepare to execute the operations within a given COA or during execution of a COA. In developing collection requirements, analysts must remember that the adversary's options are not limited to the most likely and worst case COAs identified during the IPOE process and that an adversary may opt for a different COA from the list of identified COAs or may select a COA which was not identified during the IPOE process.

In the context of intelligence support to supply chain risk management, analysts should evaluate the assessed actions an adversary must take to execute the most likely and worst case

COAs, develop a set of intelligence indicators that would identify adversary planning, preparation, and/or execution of those COAs, and then develop a collection plan to monitor those indicators. For example, if it is assessed that an adversary intends to introduce faulty/counterfeit parts into a weapon system supply chain, intelligence indicators might include adversary manufacturing of the faulty/counterfeit parts, adversary monitoring of the location or locations it is assessed that adversary might use to introduce the parts, and rigid quality inspections of parts in the supply chain to detect the introduction of faulty or counterfeit parts.

IV. Managerial Implications and Future Research

Managerial Implications

As US firms continue to seek low cost raw materials, manufacturing, and services providers in the global economy, the supply chains of those firms will continue to reach outside the borders of the US. With this expansion, comes both opportunity and risk. This trend and its accompanying risks and opportunities impacts the US defense industry and by extension, the US military. Defense acquisitions professionals cannot afford to either ignore these risks or to leave the analysis and management of these risks to the private sector. In particular, the analysis of supply chain risk posed by the deliberate action of states and non-state actors is a challenge which private sector risk management professionals are poorly positioned to address. Analysis of these threats to defense industry supply chains requires the unique capabilities of the US intelligence community. However, to date, the US defense acquisitions and intelligence communities have not developed the necessary policies and guidance to direct intelligence efforts to address this potential vulnerability in our supply chains.

This paper addresses this gap by providing a methodology for intelligence professionals to use to identify and analyze threats to weapon system supply chains. Instead of attempting to create an entirely new process for this analysis, this paper demonstrates how intelligence analysts can adapt the existing IPOE process established in joint and service doctrine to this intelligence problem. By viewing the supply chain as a military operation, analysts can apply existing analytical tools and training to identify potential threats, analyze adversaries' capabilities to disrupt our supply chains, and determine potential adversary COAs.

Future Research

While this paper provides a basic methodology for analysts to provide intelligence support to supply chain risk management, there are a number of areas which require additional research. In particular, some of the key challenges for analysts will be identifying the critical nodes and links in a supply chain and determining the most efficient use of intelligence resources to collect intelligence on these links. Additionally, determining the best sources of information regarding the nodes and links in a supply chain, their operating environment, and the relevant characteristics of the environment will be uniquely challenging as this area will often involve not only traditional intelligence targets such as government and military agencies, but also private firms and individuals. Finally, because US defense industry supply chains span political boundaries and involve both US persons and corporations as well foreign corporations and individuals, the role of intelligence oversight and the integration of the intelligence community with the counterintelligence and law enforcement communities will be vital to effective intelligence operations. Additional research such as an expert-based Delphi study into these areas will be invaluable to developing useful policy and guidance to enable the vital intelligence support necessary to ensure resilient US weapon system supply chains.

Intelligence Support to Supply Chain Risk Management

The AFIT of Today is the Air Force of Tomorrow.

Major Charles L. Carter
Department of Operational Sciences (ENS)

ADVISOR

Major Daniel D. Mattioda, USAF, Ph.D.

Introduction:

Trends such as globalization and lean manufacturing have simultaneously lengthened the supply chains of U.S. companies and increased the brittleness of those chains. These trends have significantly impacted the U.S. defense industry due to the pressures of decreasing defense budgets and limited weapon system procurement, and export controls.

Additionally, reductions in U.S. manufacturing capability and defense contractors attempts to lower costs has led to increased out-sourcing to foreign manufacturers. These trends expose US military forces to a new asymmetric threat as they potentially allow adversaries to intentionally inject sub-standard or intentionally altered parts into DoD supply chains.

Research Focus:

Based on current academic and DoD research and guidance, develop an analytical methodology to enable effective intelligence support to USAF weapon system supply chain risk management processes.

1. What is the present state of academic and Department of Defense (DoD) thought regarding supply chain resiliency , risk management , and intelligence support to supply chain risk analysis?
2. Is there an existing methodology for analysts to apply to provide intelligence support supply chain risk analysis?
3. If not, what methodology should analysts use to provide intelligence support supply chain risk

Critical Radar Component #4 – Node 2: Sichuan Assembly Plant		
Description: Manufacturers radar sub-assembly component #4		
Characteristic	Description	Effect
Political	Plant is 60% owned by PLAF	1. Production of radar component #4 may be halted/delayed if tensions increase between US and PRC government. 2. PRC may direct production of faulty components to disrupt US supply chain
Cultural	Workers are 95% Han Chinese and staff is vetted by the Party	1. Expect workforce to be loyal to PRC 2. Difficult to conduct counterintelligence operations within facility
Economic	Plant also manufactures radar components for PLAF fighter aircraft and other customers, including some export customers	Potential exists for technology transfer from radar component #4; however, PRC radar technology is already on level with that used in component
Military	Plant is 60% owned by PLAF	In the event PLAF requires additional radar components due to increase in operations tempo or aircraft production, production of radar component #4 may be halted
Criminal	Some managers/ workers in plant associated with organized crime	1. Potential exists for theft of good and/or defective radar component #4 and resale 2. Possible introduction of counterfeit goods in radar component #4 supply chain

Hypothetical Supply Chain Node Analysis

1. Define the Operational Environment
2. Describe the Operational Environment's Effects
3. Evaluate the Adversary
4. Determine the Adversary's Course of Action

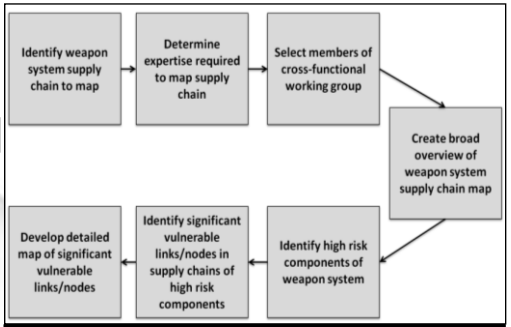
Intelligence Preparation of the Operational Environment (JP 2-1.03, AFPAM 14-118)

Contributions:

1. Identified a gap in DoD acquisitions policy regarding intelligence support to supply chain risk management
2. Developed a tailored process for analysts to use to support supply chain risk management using the Intelligence Preparation of the Operational Environment process established in Joint doctrine

Future Research Opportunties

1. What is the most effective strategy for identifying the critical links and nodes in a supply chain?
2. What are the best sources of information regarding the nodes and links in weapon system supply chains?



Focused Supply Chain Mapping Approach

Sponsor:
AFMC Intelligence Squadron

Appendix B

Vita

Major Charles Carter entered the Air Force in May 2000 upon graduation from the ROTC program at Louisiana State University where he earned Bachelor of Arts degrees in History and Russian Area Studies. He is a career intelligence officer and a United States Air Force Weapons School graduate with extensive experience executing flying and intelligence operations in CENTCOM, PACOM, and EUCOM. In addition, Maj Carter has significant experience developing and implementing unit intelligence policy and programs at the MAJCOM level.

Major Carter served in Operation SOUTHERN WATCH with the 963rd Expeditionary Air Control Squadron and in both Operation SOUTHERN WATCH and Operation IRAQI FREEDOM with the 14th Expeditionary Fighter Squadron in Saudi Arabia. Additionally, he served in Operation ENDURING FREEDOM and Operation IRAQI FREEDOM as the 379th Air Expeditionary Wing's Mission Planning Cell Chief and the Chief of Air and Air Defense Analysis at the 609th Air Operations Center in Qatar. Maj Cater's most recent duty assignment was Director of Operations, 6th Intelligence Squadron, 480th ISR Wing, Air Force ISR Agency, 7th Air Force, Osan Air Base, Republic of Korea. Major Carter is married to the former Pamela J. McGough. They have two children, Thomas, 4, and Laura, 3.

Bibliography

Associated Press. (2011, November 8). *Chinese 'are flooding Pentagon supply chain with counterfeit electronic parts and putting U.S. military at risk'.* Retrieved April 19, 2012, from Daily Mail Online: http://www.dailymail.co.uk/news/article-2058849/Chinese-counterfeit-electronic-parts-putting-U-S-military-risk.html

Bell, L. (2012, April 15). *China's Rare Earth Metals Monopoly Needn't Put An Electronics Stranglehold On America.* Retrieved May 3, 2012, from Forbes.com: http://www.forbes.com/sites/larrybell/2012/04/15/chinas-rare-earth-metals-monopoly-neednt-put-an-electronics-stranglehold-on-america/

Blackhurst, J., Dunn, K. S., and Craighead, C. W. (2011). An Empirically Derived Framework of Global Supply Resiliency. *Journal of Business Logistics*, *32* (4), 374-391.

Carter, E. E. (1972). What Are the Risks in Risk Analysis? *Harvard Business Review*, 72-82.

Christopher, M., and Lee, H. (2004). Mitigating Supply Chain Risk Through Improved Confidence. *International Journal of Physical Distribution and Logistics Management*, *34* (5), 388-396.

Christopher, M., and Peck, H. (2004a). Building the Resilient Supply Chain. *International Journal of Logistics Management*, *15* (2), 1-13.

Christopher, M., and Peck, H. (2004b). The Five Principles of Supply Chain Resilience. *Logistics Europe*, 17-21.

Cooper, M. C., and Gardner, J. T. (2005). Map Your Supply Chain. *CSCMP Explores*, 1-16.

Defense Acquisition University. (2012, January 10). *Defense Acquisition Guidebook.* Retrieved April 19, 2012, from Defense Acquisition University: https://acc.dau.mil/adl/en-US/350719/file/49150/DAG_01-10-2012.pdf

Defense Acquisition University. (n.d.). *Risk Management*. Retrieved 04 23, 2012, from Defense Acquisition University: https://acc.dau.mil/rm

Department of Defense. (2007, November 20). *DODD 5000.01 The Defense Acquisition System.* Retrieved April 17, 2012, from Defense Acquisition University: http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf

Department of Defense. (2008, December 8). *DODD 5000.02 Operation of the Defense Acquisition System.* Retrieved April 18, 2012, from Defense Acquisition University: http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf

Department of Defense. (1994, March). *DoDD 5200.1-M Acquisition Systems Protection Program.* Retrieved April 23, 2012, from Defense Technical Information Center: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA280206

Department of Defense. (2010, December 28). *DoDD 5200.39 Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection, Change 1.* Retrieved April 23, 2012, from Defense Technical Information Center: http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

Department of Defense. (2006, August). *Risk Management for DoD Acquisition.* Retrieved April 23, 2012, from Defense Acquisition University: http://www.dau.mil/pubs/gdbks/docs/RMG%206Ed%20Aug06.pdf

Department of the Air Force. (2005, January 10). *AFI 14-111 Intelligence in Force Modernization.* Retrieved April 23, 2012, from Air Force Electronic Publishing: http://www.e-publishing.af.mil/shared/media/epubs/AFI14-111.pdf

Department of the Air Force. (2008, November 25). *AFI 14-124 Predictive Battlespace Awareness (PBA).* Retrieved April 24, 2012, from Air Force Electronic Publishing: http://www.e-publishing.af.mil/shared/media/epubs/AFI14-124.pdf

Department of the Air Force. (2008, March 10). *AFPAM 14-118 Predictive Battlespace Awareness: Air and Space Intelligence Preparation of the Operational Environment.* Retrieved April 24, 2012, from Air Force Electronic Publishing: http://www.e-publishing.af.mil/shared/media/epubs/AFPAM14-118.pdf

Department of the Air Force. (2004, April 2). *AFPD 14-1 Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations.* Retrieved April 24, 2012, from Air Force Electronic Publishing: http://www.e-publishing.af.mil/shared/media/epubs/AFPD14-1.pdf

Department of the Air Force. (1998). *Air Force Handbook 32-4014, Volume 4: USAF Ability to Survive and Operate Procedures in a Nuclear, Biological and Chemical (NBC) Environment.* Washington, D.C.: Department of the Air Force.

Farris, M. T. (2010). Solutions to Strategic Supply Chain Mapping Issues. *International Journal of Physical Distribution and Logistics Management, 40* (3), 164-180.

Fiksel, J. (2006). Sustainability and Resilience: Toward a Systems Approach. *Sustainability: Science, Practice & Policy, 2* (2), 1-8.

Gardner, J. T., and Cooper, M. C. (2003). Strategic Supply Chain Mapping Approaches. *Journal of Business Logistics, 24* (2), 37-64.

Ghoshal, S. (1987). Global Strategy: An Organizing Framework. *Strategic Management Journal, 8* (5), 425-40.

Giunipero, L. C., and Eltantawy, R. A. (2004). Securing the Upstream Supply Chain: A Risk Management Approach. *International Journal of Physical Distribution and Logistics Management, 34* (9), 698-713.

Hamel, G., and Valikangas, L. (2003). The Quest for Resilience. *Harvard Business Review*, 52-63.

Haywood, M., and Peck, H. (2004). Improving the Management of Supply Chain Vulnerability in UK Aerospace Manufacturing. Retrived April 2, 2012, from http://my.fit.edu/~dkirk/4291/Lectures/EUROMAPAPER2.pdf

Hennigan, W. J. (2011, August 7). *Sky-High Overruns, Safety Ills Plague Jet.* Retrieved April 28, 2012, from Los Angeles Times: http://articles.latimes.com/2011/aug/07/business/la-fi-fighter-jets-grounded-20110807

Humphries, A. S., and Wilding, R. (2004). UK Defence Supply Chain Relationships: A Study of Sustained Monopoly. *Management Decision, 42* (2), 259-276.

Joint Chiefs of Staff. (2007). *Joint Publication 2-0: Joint Intelligence.* Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff. (2009, June 16). *JP 2-01.3 Joint Intelligence Preparation of the Operational Environment.* Retrieved April 24, 2012, from Joint Doctrine, Education, and Training Electronic Information System: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=220

Kendall, F. (2012, March 16). Overarching DoD Counterfeit Prevention Guidance. *Memorandum* . Washington, D.C.: Under Secretary of Defense.

Krekel, B., Adams, P., and Bakos, G. (2012). *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage.* U.S.-China Economic and Security Review Commission. Northrup-Grumman.

Lambert, D. M., and Cooper, M. C. (2000). Issues in Supply Chain Management. *Industrial Marketing Management, 29*, 65-83.

Manuj, I., and Mentzer, J. T. (2008a). Global Supply Chain Risk Management. *Journal of Business Logistics, 29* (1), 133-155.

Manuj, I., and Mentzer, J. T. (2008b). Global Supply Chain Risk Management Strategies. *International Journal of Physical Distribution and Logistics Management, 38* (3), 192-223.

Merriam-Webster. (n.d.). *Risk*. Retrieved March 27, 2012, from Merriam-Webster: http://www.merriam-webster.com/dictionary/risk

Norrman, A., and Jansson, U. (2004). Ericsson's Proactive Supply Chain Risk Management Approach After a Serious Sub-Supplier Accident. *International Journal of Physical Distribution &Logistics Management, 34* (5), 434-456.

Peck, H. (2005a). Drivers of Supply Chain Vulnerability: An Integrated Framework. *International Journal of Physical Distribution & Logistics Management, 35* (4), 210-229.

Peck, H. (2005b). *Reducing Risk in the Defence Supply Chain.* Retrieved 03 28, 2012, from Defence Management: http://www.defencemanagement.com/article.asp?id=175&content_name=Procurement%20and%20Material%20Management&article=4246

Pettit, T. J. (2008). *Supply Chain Resilience: Development of a Conceptual Framework, an Assessment Tool, and an Implementation Process.* Columbus, OH: Ohio State University.

Pettit, T. J., Fiksel, J., and Croxton, K. L. (2010). Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *Journal of Business Logistics, 31* (1), 1-21.

Pickett, C. (2006). Prepare for Supply Chain Disruptions Before They Hit. *Logistics Today, 47* (6), 22-24.

President of the United States. (2012). *National Strategy for Global Supply Chain Security.* Washington, D.C.: Office of the President of the United States.

Price Waterhouse Coopers. (2009, January). *How to Fortify Your Supply Chain Through Collaborative Risk Management.* Retrieved April 4, 2012, from PWC.com: http://www.pwc.com/us/en/aerospace-defense/assets/pwc-aerospace-scrm-012008-rdt.html

Svensson, G. (2000). A Conceptual Framework for the Analysis of Vulnerability in Supply Chains. *International Journal of Physical Distribution and Logistics Management, 30* (9), 731-750.

Tobin, B. P. (2011). Supply Chain Resilience: Assessing USAF Weapons System Life Cycle. Wright-Patterson Air Force Base, OH: Air Force Institute of Technology.

Undersecretary of Defense for Acquisitions, Technology, and Logistics. (2010, October 6). *Directive-Type Memorandum (DTM) 10-015 - Requirements for Life Cycle.* Retrieved April 18, 2012, from Defense Acquisitions University: https://dap.dau.mil/policy/Documents/Policy/USA005479-10%20DTM%20%2010-015.pdf

Undersecretary of Defense for Acquisitions, Technology, and Logistics. (2011, July 18). *Document Streamlining - Program Protection Plan (PPP).* Retrieved April 18, 2012, from Defense Acquisitions University: https://dap.dau.mil/policy/Lists/Policy%20Documents/Attachments/3298/USA003781-11_Signed.pdf

Webster, J., and Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26* (2), xiii-xxiii.

Zsidisin, G. A., Panelli, A., and Upton, R. (2000). Purchasing Organization Involvement in Risk Assessments, Contingency Plans, and Risk Management: An Exploratory Study. *Supply Chain Management: An International Journal*, *5* (4), 187-198.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
14-06-2012	**Graduate Research Project**	May 2011 – Jun 2012

4. TITLE AND SUBTITLE

Intelligence Support to Supply Chain Risk Management

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Carter, Charles L., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Street, Building 641
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ILS/ENS/12-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Materiel Command Intelligence Squadron
Attn: Lt Col Steven Gorski
2450 D St
Wright-Patterson AFB, OH. 45433
(937) 656-7568 (DSN: 986-7568) e-mail: Steven.Gorski@wpafb.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFMC IS/CC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research was to improve defense supply chain risk management processes through better intelligence integration. To this end, this research sought to capture the present state of academic and Department of Defense (DoD) thought regarding supply chain resiliency and risk management through an extensive review of current academic and DoD literature regarding supply chain risk management and intelligence doctrine. This review established the importance of supply chain risk analysis to ensuring supply chain resiliency and identified a significant gap in DoD acquisitions policy and guidance regarding intelligence support to supply chain risk analysis.

This research culminated in the development of a methodology for intelligence professionals to use to support supply chain risk management processes. Specifically, this paper provides analysts a methodology to provide intelligence support to risk analysis for United States Air Force (USAF) weapon system supply chains based on the Intelligence Preparation of the Operational Environment process established in Joint doctrine. While the methodology developed in this paper is targeted at USAF weapon system supply chains, it is readily adaptable to other DoD acquisitions program supply chains. Additionally, this paper provides recommendations for future research to further improve intelligence support to supply chain risk management.

15. SUBJECT TERMS

Supply Chain Management, Risk Management, Risk Analysis, Intelligence, Acquisitions, Sustainment, Supply Chain Resiliency

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Daniel D. Mattioda, Major, USAF, Ph.D. (ENS)
U	**U**	**U**	**UU**	78	**19b. TELEPHONE NUMBER** *(Include area code)* 937-255-3636, Ext. 4510; e-mail: daniel.mattioda@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18